

INFORMATION LAW IN THE NEW PARLIAMENT¹

Timothy Pitt-Payne QC

1. The May 2010 General Election has been followed by the formation of a coalition Government between the Conservatives and the Liberal Democrats.
2. The principal policies of the new Government are set out in two documents, collectively referred to as the Coalition Programme for Government. The first is an agreement between the coalition parties, dated 11th May 2010. The second, more detailed document is entitled “The Coalition: our programme for government”, published on 20th May.
3. There are three other documents, all published on 21st May 2010 and available via the 10 Downing Street website², that may be of interest to those seeking to understand how the new Government will work:
 - a revised version of the Ministerial Code;
 - a list of Cabinet committees and their membership; and
 - the “Coalition Agreement for Stability and Reform”, explaining the practical arrangements for how the two parties will work together.
4. Before discussing the Coalition’s programme for Government, I set out some background about political and legal developments during the last Parliament relating to information law.

THE POLITICS OF INFORMATION LAW 2005-2010

5. During the last Parliament (2005-2010) information law issues moved up the political agenda at a rapid pace. There was increasing debate about the public right to know, but also about the right to protection for private information.

¹ This is an updated version of a paper given to the 11KBW Information Law seminar on 19th May 2010.

² <http://www.number10.gov.uk/news/latest-news/2010/05/ministerial-codgovernment-unveils-mini-50501>

6. As far as the right to know is concerned, the Freedom of Information Act 2000 (“FOIA”) and the Environmental Information Regulations 2004 (“EIR”) came fully into force on 1st January 2005. They have now become an established part of the political landscape, and the new Government is committed to strengthening the regime for access to public sector information. As discussed below, the new Government also has a number of proposals for the routine dissemination of information held by public authorities.
7. Over the past 5 years there have been a series of high-profile cases arising out of FOIA requests, involving matters such as: central Government information about education policy³; MPs’ expenses⁴; childhood leukaemia statistics for an area of extensive nuclear activity⁵; and the decision to go to war in Iraq⁶. On two occasions, the Government has exercised its statutory right of veto⁷. It is now commonplace to see newspaper stories that are based on FOIA or EIR requests.
8. It is unsurprising that FOIA should have proved significant in political terms. What is perhaps more striking is the way in which data protection and information privacy have also become matters of public debate. Only a few years ago these would have been widely regarded as marginal subjects, of interest only to specialists. But consider the following passage, from a 2009 *Guardian* article⁸:

There's no easy prescription, but here's an idea for debate. In the database society, the information commissioner will be one of the main bastions of defence against excesses by the state and private enterprise. Should not the post become a directly elected one? The issue already attracts a high level of public interest – the 1998 Data Protection Act is the best selling act of parliament – and this will surely increase. It's not impossible to envisage an election for information commissioner achieving a higher turnout than those for many Westminster constituencies. Such a mandate would attract ambitious political figures who fancy themselves as having an ear to the ground. Boris for commissioner?

³ *DfES v Information Commissioner* EA/2006/0006

⁴ See e.g. *Corporate Officer of the House of Commons v Information Commissioner* [2008] EWHC 1084 (Admin)

⁵ *Common Services Agency v Scottish Information Commissioner* [2008] UKHL 47

⁶ *Cabinet Office v Information Commissioner* EA/2008/0024

⁷ In relation to the minutes of the pre-Iraq war Cabinet discussions: <http://www.justice.gov.uk/news/docs/foi-certificate-section53-foi-act-2000.pdf>; and in relation to disclosure of the minutes of a 1997 Cabinet ministerial committee on devolution: <http://www.justice.gov.uk/news/docs/section53-certificate.pdf>

⁸ *Guardian* 14th May 2009, Michael Cross.

9. The changing attitude of the Conservative party is a good yardstick. In August 2007 the party published a report⁹ by its Economic Competitiveness Policy Review Group, chaired by John Redwood MP (not a member of the new Cabinet). Paragraph 6.10 included the following statement:

Data Protection. *We recommend the repeal of this expensive bureaucracy, which fails to protect people's data. The ever growing power of the internet and computers means we all end up on ever more lists, whether we want to or not. Proper handling of the data given to public bodies and private sector companies would be governed by the general law of privacy, and by established codes of conduct.*

Compare the notorious words of Scott McNealy, CEO of Sun Microsystems, in January 1999: "You have zero privacy anyway. Get over it."¹⁰

10. By contrast, in September 2009 Dominic Grieve (then Shadow Justice Secretary, and now Attorney General) launched a policy paper entitled "Reversing the Rise of the Surveillance State"¹¹. Among a list of 11 measures to protect privacy and hold government to account, the report proposed that the audit powers and independence of the Information Commissioner should be strengthened, that the Commissioner should have a wider role in relation to data security, and that Home Office plans regarding communications data should be submitted to the Commissioner for pre-legislative scrutiny.
11. So, in the eyes of the Conservative party, by the time of the 2010 General Election data protection legislation and the Information Commissioner were no longer regarded as regulatory burdens on business. Instead they were seen as essential to protect individual liberties against an overbearing central State.
12. What changed between summer 2007 and autumn 2009? One obvious answer is that in November 2007 HMRC announced¹² that it has lost the child benefit records of 25 million people.

⁹ See <http://www.conservatives.com/pdf/ECPGcomplete.pdf>

¹⁰ See <http://www.wired.com/politics/law/news/1999/01/17538>

¹¹

http://www.conservatives.com/News/News_stories/2009/09/~/_media/Files/Policy%20Documents/Surveillance%20State.ashx

¹² See <http://news.bbc.co.uk/1/hi/7103566.stm>

Suddenly, concerns about how securely personal information was held by the public sector were on the front pages of the newspapers.

13. Alongside this increased concern about information security, there has been a focus on both the amount of personal data held by public authorities, and the very wide range of uses to which it is put. Two phrases became commonplace: that we are living in a “surveillance society”, or heading that way; and that the “database state” is over-mighty and needs to be restrained. Milestones in this debate include the following.

- The report on the Surveillance Society, commissioned by the ICO from the Surveillance Studies network, and published in September 2006¹³.
- The Convention on Modern Liberty, in February 2009: one of the sessions discussed the database state¹⁴.
- The Joseph Rowntree Trust report on the Database State, published in March 2009¹⁵.
- The September 2009 Conservative policy paper, referred to above.

14. Developments that are sometimes said to be manifestations of a surveillance society or database state include the following:

- the ID cards project;
- the maintenance or creation within the public sector of large databases of personal information;
- the widespread collection and retention of DNA information by the police;
- covert surveillance by public authorities;
- data sharing initiatives within the public sector;

¹³ http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf

¹⁴ See <http://www.modernliberty.net/2009/the-database-state>

¹⁵ <http://www.jrrt.org.uk/uploads/Database%20State.pdf>

- the collection of information about telephone, email and internet usage;
- comprehensive vetting of those working with children or vulnerable adults; and
- the increasing use of CCTV.

15. As the above list illustrates, the debate has tended to focus on the way that personal information is collected and used by public authorities. But there also increasing awareness of the very large amount of information that is collected by the private sector. The recent controversies about Google Streetview and about Facebook's privacy policies are a good illustration¹⁶.

16. These developments in political debate have coincided with important new case-law from the Courts, balancing the right to information privacy against other social goals.

- In *L v Commissioner of Police of the Metropolis* [2009] UKSC 3, the Supreme Court held that the disclosure of non-conviction information in the context of enhanced CRB disclosures would usually engage article 8 of the Convention; and that there could be no general assumption that privacy would always give way to child protection considerations¹⁷.
- In the *Marper* litigation the ECHR¹⁸ took a radically different approach from the House of Lords¹⁹, and held that the UK's DNA database contravened article 8, because DNA samples and profiles (and also fingerprints) were retained indefinitely even from those not convicted of any offences.
- By contrast, in *Chief Constable of Humberside Police and others v Information Commissioner* [2009] EWCA Civ 1079, the Court of Appeal overturned enforcement notices issued by the Commissioner that required certain old, minor convictions to be deleted from the Police National Computer: the Court considered that it was particularly important for a comprehensive record of convictions to be available to the criminal courts, e.g. for sentencing purposes.

¹⁶ See http://www.economist.com/displayStory.cfm?story_id=16163396 (*Economist*, 20th May 2010)

¹⁷ The Supreme Court therefore disapproved of the approach taken in *X v Chief Constable of the West Midlands Police* [2004] EWCA Civ 1068

¹⁸ *S and Marper v UK* (Applications nos 30562/04 and 30566/04, judgment 4th December 2008)

¹⁹ [2004] UKHL 39

LEGISLATIVE DEVELOPMENTS 2005-2010

17. The key legislation dates from the first Blair government (1997-2001): the Data Protection Act 1998 (“DPA”); the Freedom of Information Act 2000; the Human Rights Act 1998 (“HRA”); and the Regulation of Investigatory Powers Act 2000 (“RIPA”). But there were some significant further developments during the last Parliament, including legislation passed during the “wash up” at the end of the Parliamentary term.
18. The Coroners and Justice Act 2009, when first introduced as a Bill, included provisions to amend the DPA so as to facilitate information sharing. These provisions (originally clause 152 of the Bill) were withdrawn in March 2009 in the face of concerned opposition, including from the British Medical Association, civil liberties groups, and the Bar Council. However, more modest proposals for information sharing continued to be put forward. For instance, on 5th March 2010 the Department of Health launched a consultation²⁰ on proposed regulations imposing a “duty of co-operation” on healthcare organisations, requiring them to share information about the conduct or performance of health care workers in order to protect patient safety. The consultation period has been extended to 9th July 2010: whether the proposals are taken forward by the new Government remains to be seen.
19. Various changes were made to FOIA by the Constitutional Reform and Governance Act 2010: see section 46 of and Schedule 7 to the Act. In particular:
- The exemption in section 37(1) of FOIA (relating to communications with the Sovereign and with other members of the Royal Family) was extended. In relation to the Sovereign and the heir to the Throne, the exemption was made absolute²¹.
 - The period at which a record becomes a “historical record” was altered. Under FOIA as originally enacted, a record became a historical record at the end of 30 years beginning with the year following that in which it was created: see FOIA section 62(1). Information contained in a historical record could be exempt by virtue of sections 28, 30(1), 32, 33, 35, 36, 37(1)(a), 42 or 43: see FOIA section 63(1). Under the 2010 Act the period of 30 years is reduced to 20 years²². Provision is made for a 10 year transitional period in introducing this

²⁰ See http://www.dh.gov.uk/en/Consultations/Liveconsultations/DH_113563

²¹ See Schedule 7, paragraph 3

²² See Schedule 7 paragraph 4(2)

change²³. However, in respect of section 36 (so far as it relates to certain information concerning Northern Ireland), section 28, or section 43, the time after which these exemptions can no longer be relied upon will remain 30 years not 20 years²⁴.

20. These changes have not yet been brought into force. It remains to be seen whether they will be implemented by the new Government.

21. In relation the DNA database, the Crime and Security Act 2010 (sections 14-23) provided for a retention period of up to 6 years for DNA profiles and fingerprints taken from persons not subsequently convicted of an offence.

22. The Safeguarding Vulnerable Groups Act 2006 creates a new vetting and barring regime for those working with children and vulnerable adults. The Act came into force in stages: from 12th October 2009 the three former barring lists²⁵ were replaced by two new lists, one relating to children and the other relating to vulnerable adults. The new Independent Safeguarding Authority (ISA) will be responsible for maintaining the list. The requirement for those working with children or vulnerable adults to be ISA-registered is due to be phased in, from July 2010 onwards. The potential scope of the ISA regime has proved controversial, with media reports that over 9 million adults would eventually need to register under the scheme²⁶.

INFORMATION LAW AND THE COALITION AGREEMENT

23. The coalition Government therefore takes office against a background where:

- rights of access to public sector information are widely taken for granted; and
- there is increasing concern about the volume of information that the State holds about individuals, the security of that information, and the use to which it is put.

²³ See section 46(2) of the 2010 Act, read with Schedule 7 paragraph 4.

²⁴ See Schedule 7 paragraph 5.

²⁵ I.e. under section 142 of the Education Act 2002; section 1(1) of the Protection of Children Act 1999; and Part 7 of the Care Standards Act 2000 (vulnerable adults).

²⁶ See e.g. <http://www.prospectmagazine.co.uk/2010/03/why-child-protection-has-gone-too-far/> (*Prospect*, issue 169).

The future of the HRA

24. One immediate question is the new Government's likely approach to the HRA. Of course this has significance for a very wide range of issues, going well beyond information law. In the present context article 8 of the Convention is particularly important, because of its role in protecting privacy rights in relation to personal information.
25. The Coalition parties have in the past taken very different approaches to the HRA. The Conservative manifesto²⁷ (page 79) promised to replace the HRA with a UK Bill of Rights. The Liberal Democrats²⁸ in their manifesto (page 94) promised to protect the HRA.
26. Since the Coalition was formed there have been mixed messages about the HRA's future. The new Justice Secretary (and Lord Chancellor), Kenneth Clarke MP, had previously described the proposal to replace the HRA with a home-grown Bill of Rights as "xenophobic and legal nonsense": his appointment was widely viewed as an indication that proposals to replace the HRA had been abandoned²⁹. However, controversy over the HRA was revived shortly afterwards by the decision of the Special Immigration Appeals Commission on 18th May 2010 that a number of suspected terrorists could not be deported to Pakistan³⁰ because of the need to protect their rights under article 3 of the Convention.
27. The Coalition's programme for government, published on 20th May 2010 ("the Programme") includes the following passage (in the section about Civil Liberties: page 11).

We will establish a Commission to investigate the creation of a British Bill of Rights that incorporates and builds on all our obligations under the European Convention on Human Rights, ensures that these rights continue to be enshrined in British law, and protects and extends British liberties. We will seek to promote a better understanding of the true scope of these obligations and liberties.

²⁷ "Invitation to Join the Government of Britain", available online at http://media.conservatives.s3.amazonaws.com/manifesto/cpmanifesto2010_lowres.pdf

²⁸ Manifesto available here: http://network.libdems.org.uk/manifesto2010/libdem_manifesto_2010.pdf

²⁹ See e.g. <http://www.telegraph.co.uk/news/newstoppers/politics/conservative/7721590/Coalition-government-Conservatives-drop-plans-to-scrap-European-Human-Rights-Act.html> (*Telegraph*, 14th May 2010).

³⁰ See the BBC website coverage on 18th May 2010: <http://news.bbc.co.uk/1/hi/uk/8690572.stm>

This does not suggest any appetite for immediate change to the HRA. Whatever the outcome of the proposed Commission, the importance of article 8 in UK law is unlikely to be diminished.

Increasing the transparency of Government

28. Section 16 of the Programme (page 20) is headed “Government Transparency”. Much of this is taken up with commitments that certain categories of information will regularly be made public. According to the introduction to the “Government Transparency” section, these proposals are intended to help hold politicians and public bodies to account, and also to assist in achieving better value for money and in cutting the deficit. . Elsewhere in the Programme there are a number of other proposals for the routine publication of information.
29. In all, there are at least 15 separate commitments relating to the regular publication of various categories of information.
- (i) Public bodies will be required to publish online the job titles of every member of staff and the salaries and expenses of senior officials paid more than the lowest salary permissible in Pay Band 1³¹ of the Senior Civil Service pay scale (pp 20-21).
 - (ii) Steps will be taken to open up government procurement, and government ICT contracts will be published online (page 21).
 - (iii) Full online disclosure will be required for all central government spending and contracts over £25,000 (page 21).
 - (iv) Councils will be required to publish meeting minutes and local services and performance data (page 21).
 - (v) Councils will be required to publish items of spending above £500 and to publish contracts and tender documents in full (page 21).
 - (vi) Small business procurement is to be promoted, in particular by introducing an aspiration that 25% of government contracts should be awarded to small and medium-sized businesses and by publishing government tenders in full online and free of charge (page 10).

³¹ This currently begins at £58,200: <http://www.civilservice.gov.uk/jobs/Entry/Experienced-Professionals/scs-pay.aspx>

- (vii) The Sustainable Communities Act will be implemented so that citizens' know how taxpayers' money is spent in their area³² (page 12).
- (viii) The police will be obliged to publish detailed local crime statistics each month (see page 13).
- (ix) Serious case reviews will be published, with identifying details removed (page 20).
- (x) Details of all UK aid spending will be published online (page 22).
- (xi) Detailed data will be published online about the performance of healthcare providers (page 25).
- (xii) Details will be published of every UK project that receives over £25,000 of EU funds (page 27).
- (xiii) Performance data on education providers will be published, as will past exam papers (page 29).
- (xiv) Further information will be published about the costs, graduate earnings and student satisfaction ratings of different university courses (page 32).
- (xv) There will be a new public reading stage for Bills: there will be an opportunity for the public to comment on proposed legislation online, and a dedicated "public reading day" where those comments will be debated by the committee scrutinising the Bill (page 27).

30. Thus as far as public sector contracts are concerned, the intention seems to be that the full terms of the following should be published online: government ICT contracts; central government contracts worth over £25,000; and local authority contracts worth over £500. At present this information can be requested under FOIA/EIR or (in some circumstances) under the Audit Commission Act 1998, but public authorities and their private sector contractors often resist the full disclosure of contractual terms. For instance, in *Department of Health v Information Commissioner* (EA/2008/0018) the Tribunal considered a request for disclosure of a contract for the provision of an electronic recruitment service for the NHS. The Department sought to

³² Section 6 of this Act provides for the production of local spending reports by the Secretary of State. The first such report was published on 29th April 2009 and is available here: <http://www.communities.gov.uk/publications/localgovernment/localspendingreports200607> A consultation paper on a proposed second report was published on 30th March 2010 and is available here: <http://www.communities.gov.uk/documents/communities/pdf/1525070.pdf>

withhold the contract wholly or in part, relying on FOIA sections 41, 43 and 44. The Tribunal held that the contract should be disclosed in part. In *Veolia v Nottinghamshire County Council and others* [2009] EWHC 2382 (Admin), a private sector contractor unsuccessfully challenged (by way of judicial review) a local authority's decision to disclose part of the contract between them, under the Audit Commission Act 1998³³.

31. There is also a proposal in the Programme for the publication of tender documents online in relation to local authority expenditure over £500, and (possibly) in relation also to one or more of the following: (i) central government contracts worth over £25,000; (ii) ICT contracts; (iii) central government contracts generally. It is not clear though exactly what information is to be published. Is it simply the documentation issued by the public authority in connection with the tendering process? Or is it also the bid documentation produced by the tenderers themselves? If the latter is to be published, at what stage will this take place: before or after completion of the tendering process?
32. Disclosure of bid documentation produced by tenderers is often requested under FOIA, but there are a number of potential restrictions on its disclosure. There are numerous FOIA exemptions that may be applicable, including those in sections 41 (information received in confidence), section 43 (commercial interests) and section 44 (statutory prohibitions on disclosure).
33. As far as section 44 is concerned, there is a relevant prohibition in regulation 43 of the Public Contracts Regulations 2006, as follows:

(1) Subject to the provisions of these Regulations, a contracting authority shall not disclose information forwarded to it by an economic operator which the economic operator has reasonably designated as confidential.

(2) In this regulation, confidential information includes technical or trade secrets and the confidential aspects of tenders.

This reflects the provisions of EU procurement law: see e.g. Directive 2004/18/EC, article 6. The European Court of Justice has emphasised the importance of proper protection for the confidentiality of information provided by tenderers: see the *Varec* case (C-450/06, judgment of 14th February 2008). The EU procurement regime will be a significant constraint on any proposals for widespread routine disclosure of information provided by tenderers.

³³ The case will be heard by the Court of Appeal in July 2010.

34. The Office of Government Commerce has given extensive guidance about the application of FOIA in relation to civil procurement³⁴. In the *Department of Health* case the Tribunal indicated (see at §87) that in future it would expect to see a clear explanation for any departure by public authorities from these guidelines. Clearly the OGC guidelines are likely to require substantial revision when the Government's proposals are implemented.

Facilitating the commercial exploitation of Government information

35. The "Government Transparency" section of the Programme also indicates that the Government is seeking to facilitate the commercial exploitation of public sector information. The heading of this section (page 20) states that:

Setting government data free will bring significant economic benefits by enabling businesses and non-profit organisations to build innovative application and websites.

36. In order to achieve this, there is to be a new "right to data" so that Government-held datasets can be requested and used by the public and then published on a regular basis (page 21). All data published by public bodies will be published in an open and standardised format so that it can be used easily and with minimal cost by third parties (page 21).

37. These commitments reflect the Conservative manifesto: see page 69 of the manifesto, where a figure of £6 billion was quoted for the potential boost that measures of this kind could give to the UK economy.

38. What is unclear is how these proposals will fit into the existing legal framework. There are a number of questions. In what way will the new right to data differ from the existing right of access to information under FOIA section 1? For instance, will there be a right to request that particular datasets should be regularly published (as compared to the FOIA right, which is simply to request the information that is held at the time of the request)? And what (if any) costs limits will be applied to the new right? Will everybody be entitled to take advantage of the new right to data, or will it only be for those intending to make commercial use of the data? For instance, will journalists be able to make use of this right?

³⁴ See the November 2008 guidance, at http://www.ogc.gov.uk/documents/OGC_FOI_and_Civil_Procurement_guidance.pdf See also the material on the Ministry of Justice website here: <http://www.justice.gov.uk/guidance/foi-assumptions-procurement.htm>

39. It is also unclear how this new right will interact with the Re-use of Public Sector Information Regulations 2005.

Extending the scope of FOIA

40. As well as the various proposals discussed above, section 3 of the Programme (dealing with Civil Liberties) also includes a general commitment to extend the scope of FOIA in order to provide greater transparency: see page 11.

41. The Conservative manifesto did not include any specific commitments about FOIA. It focused on proposals for the routine disclosure of information, along the lines discussed in the previous section of this paper. The Liberal Democrat manifesto promised a Freedom Bill, a draft of which is available online: see <http://freedom.libdems.org.uk/the-freedom-bill/full-text-of-the-freedom-bill/> Part 5 deals with Freedom of Information. Three specific amendments are proposed:

- in section 36 of FOIA, a test of “substantial prejudice” rather than “prejudice”;
- the repeal of the Ministerial veto in FOIA section 53; and
- a right of appeal from the Tribunal, not confined to appeals on a point of law (amending FOIA section 59).

42. These proposals have their puzzling aspects. For instance, it is not clear what practical difference the proposed change to section 36 would make, or why no similar change is proposed for the other prejudice-based exemptions. And few users of the Act, one suspects, would identify the limited scope of appeals from the Tribunal as being a priority for reform.

43. There is no specific proposal in either manifesto, or in the Programme, for tackling the considerable delays that can be a feature of the FOIA process. For instance, there is no proposal to impose statutory time limits for the conduct of an internal review; or to give a right to refer a complaint to the Tribunal if the Information Commissioner’s investigation takes longer than a specified time.

44. Nor is there anything about ending the anomalous distinction between the remedies available to those seeking information under section 1 of FOIA, and to those making subject access requests to public authorities under DPA section 7. In many cases, a request for information will engage both regimes, and the public authority will need to deal with part of it under FOIA and the

remainder under the DPA. If there is a complaint to the Information Commissioner, only the FOIA element of the request will be handled under the complaints provision in FOIA section 50; the remainder is likely to be treated as a request for assessment under DPA section 42. And the Tribunal will only have jurisdiction in relation to the FOIA element of the request; in order to pursue the DPA element, the requester will need to make an application to the Court under DPA section 7.

45. Nor are there any promises – in the Programme, or in either manifesto – that there will be more resources for public authorities or the Commissioner so that they can give proper effect to a strengthened FOIA. But then, as we know on very good authority, there's no money left³⁵.

Information privacy and the use of personal data

46. There are a number of commitments in the Programme that are – broadly speaking – intended to protect information privacy and to limit the collection or use of personal data by public authorities. Unless otherwise stated below, these proposals are all in the Civil Liberties section of the Programme.

Scrapping ID cards, the National Identity Register, and the Contact Point Database; and halting the next generation of biometric passports

47. These commitments are self-explanatory. They are lifted almost verbatim from the Conservative manifesto (page 79), where they are linked with an attack on Labour's approach to personal privacy, as "intrusive, ineffective and enormously expensive". All of these proposals reflect the criticism of the "database state", referred to above.

Outlawing the fingerprinting of children at school without parental permission

48. This commitment directly reflects Part 5 of the Liberal Democrats' Freedom Bill, which proposed creating a power to introduce regulations governing the taking of biometric information from

³⁵ See <http://business.timesonline.co.uk/tol/business/economics/article7128665.ece>

persons under 16; the Bill envisaged that any regulations should make provision as to the gathering of parental consent.

49. Currently there is no specific regulation of the use made in schools of biometric information: in order to consider whether such use was lawful, it would be necessary to consider the general legal framework governing the use of personal information, in particular the DPA and the HRA.
50. There is relevant guidance from the Information Commissioner issued in August 2008: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fingerprinting_final_view_v1.11.pdf. This deals with matters such as the use of Automated Fingerprint Identification Systems (AFIS) for registration and other purposes. The ICO's guidance is that the DPA does *not* expressly require parental consent for the collection of biometric information from pupils; but that parents must be fully involved and informed, in order to ensure that personal data is processed fairly. Biometric information must be collected for specified purposes; must not be used for wider purposes; must be kept secure; and must be destroyed when no longer required. In particular, AFIS systems and similar technologies should not be used as a starting-point for the covert creation of a national fingerprint database.

Adopting the Scottish model for the DNA database

51. Both parties' manifestos promised to curtail the storage of DNA profiles of those who had not been convicted of any offence.
52. The Scottish model mentioned in the Programme was also referred to by the European Court of Human Rights in *Marper*, where it was found to be particularly significant in assessing the UK database: see at §§36 and 109 of the *Marper* decision.
53. Under the Scottish system the DNA samples and resulting profiles must generally be destroyed if the individual is not convicted or is granted an absolute discharge. However, biological samples and profiles may be retained for three years if the arrestee is suspected of certain sexual or violent offences even if the person is not convicted. Thereafter samples and information are required to be destroyed, unless a Chief Constable applies to a Sheriff for a two-year extension.
54. Thus what is proposed in the Programme will lead to a reduction in the retention of the DNA profiles of non-convicted individuals, as compared with the regime established by the Crime and Security Act 2010 referred to above.

Further regulation of CCTV

55. This commitment reflects a proposal in the Liberal Democrats' Freedom Bill that a Royal Commission should be established to make urgent recommendations on the use of CCTV and its impact on privacy.
56. Some local authorities have produced Codes of Practice governing the use of CCTV. The Liberal Democrats, in commentary on the draft Freedom Bill³⁶, have referred specifically to the work done by Cambridge City Council³⁷, and have suggested that a starting point for the Royal Commission would be to look at whether Codes of this kind should be given statutory force.
57. The Information Commissioner has also published a CCTV Code, last updated in 2008: see: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_cc_tvfinal_2301.pdf
58. One option for reform would be for Codes of this nature to be given statutory force in some way. For instance there might be a specific statutory obligation on CCTV users to have regard to a Code produced by the Commissioner; or to produce and publish their own codes. A more radical option might be a specific licensing regime for CCTV systems, with a power (exercisable by the Information Commissioner?) for the licence to be forfeited for breach of any statutory code of practice.

Ending the storage of internet and email records without good reason

59. This area is governed the EU Data Retention Directive (2006/24/EU) implemented in the UK by regulations in October 2007 and April 2009³⁸, imposing data retention obligations on ISPs and telecommunications providers. Access to the retained information about internet and email records is governed by the Regulation of Investigatory Powers Act 2000 (RIPA). A proposal by

³⁶ See <http://freedom.libdems.org.uk/the-freedom-bill/7-regulation-of-cctv/>

³⁷ See <http://www.cambridge.gov.uk/public/docs/CCTV%20code%20of%20practice.pdf> for the Cambridge code.

³⁸ See SI 2007/2199 available at http://www.opsi.gov.uk/si/si2007/uksi_20072199_en_1; and see SI 2009/859 available at http://www.opsi.gov.uk/si/si2009/uksi_20090859_en_1

the last Government for a Communications Data Bill was not pursued: the suggestion of a single central Government database to store information about internet and email communications was widely criticised.

60. This part of the Programme is extremely vague: it merely puts down a marker. Another Royal Commission, perhaps?

Health information

61. According to the NHS section of the Programme, the Government will put patients in charge of making decisions about their care, including control of their health records (see page 25).
62. There has been considerable debate in recent years about the way in which the NHS holds patient information, in particular in connection with the new NHS Spine database project³⁹. Clearly there is a difficult balance between allowing patients to control the way in which their health information is used, and ensuring that all health professionals have proper access to the information that they need for clinical purposes. The Programme suggests that the Government is proposing to shift the balance towards patient autonomy and control, but the details remain uncertain.

Employment vetting

63. Reference was made above to the controversial nature of the ISA vetting and barring scheme, and in particular to the wide scope of the requirement to register for monitoring with the ISA. The new ISA scheme operates alongside the CRB disclosure regime⁴⁰: standard CRB checks cover all criminal convictions (including those that are spent under the Rehabilitation of Offenders Act 1974), while enhanced CRB checks also cover non-conviction information (or “soft intelligence”) at the discretion of local police forces. Reference was made above to *L v Commissioner of Police of the Metropolis*, where the Supreme Court considered how article 8 of the Convention affected the discretion to disclose soft intelligence as part of an enhanced CRB disclosure.

64. The Programme (at page 20) states:

³⁹ See <http://www.panopticonblog.com/2010/03/26/patient-data-sharing-are-we-running-out-of-patience/>

⁴⁰ Governed by Part V of the Police Act 1997.

We will review the criminal records and vetting and barring regime and scale it back to common sense levels.

65. Elsewhere in the Programme there is a commitment to encourage volunteering and involvement in social action (see page 30: this is in the “Social Action” section of the programme). This reflects the “Big Society” theme that was (intermittently) prominent in the Conservative election campaign. The Programme does not make any explicit link between the desire to encourage volunteering, and the proposed review of the CRB/ISA regimes. This is perhaps surprising: media criticism of these regimes often focuses on their alleged effect in discouraging voluntary work.
66. In any review of the ISA/CRB regimes, I would suggest that the following issues are likely to be significant: (i) whether the definition of “regulated activity” for the purpose of the ISA scheme is too wide; (ii) whether the ISA scheme’s application to voluntary work, and in particular to activities carried out by parents in connection with their children’s school, should be cut back; and (iii) whether it is still necessary, given the ISA scheme, for soft intelligence to be made available directly to prospective employers under the CRB scheme.
67. There is also a specific commitment in the Programme (see page 24, in the “Justice” section) to change the law so that historical convictions for consensual gay sex with over-16s will be treated as spent and will not show up on CRB checks.

RIPA and surveillance

68. Surveillance by public authorities has proved highly controversial in recent years.
69. Surveillance is a potential breach of article 8 of the Convention. RIPA sets out provisions whereby various types of surveillance can be authorised. Where these provisions are followed, the surveillance will be lawful for all purposes: see RIPA section 27. This means that, in resisting a challenge under article 8 of the Convention, the public authority will be able to rely on the RIPA authorisation in order to establish that any interference with the article 8 right was “prescribed by law”. However, RIPA does not itself provide that surveillance not authorised under RIPA is unlawful. Unauthorised surveillance does not benefit from the shield provided by RIPA section 27, but whether it is actually unlawful would depend on the application of other relevant legal provisions: e.g. the HRA, the DPA, or the common law in relation to trespass.

70. The Investigatory Powers Tribunal has already narrowed the potential relevance of RIPA for local authorities, by holding that surveillance in connection with a council's employment functions will usually fall outside the scope of RIPA: see *C v Police* (14th November 2006: IPT/03/32/H)⁴¹.
71. The Programme proposes to ban the use of RIPA powers by councils, unless the use is signed off by a magistrate and required for stopping serious crime (see page 12, in the "Communities and Local Government" section). This will be a considerable limitation on the ability of local authorities to use RIPA authorisations. It remains to be seen whether the Government will go one stage further, and expressly prohibit local authority surveillance where it is not authorised under RIPA.

CONCLUSION

72. The Programme leaves considerable room for further debate about detailed implementation. But the intended direction of travel is clear.
73. The Government sees further moves towards openness and transparency as being a valuable weapon in controlling public spending. At present its emphasis seems to be more on the routine, regular disclosure of certain kinds of information, as opposed to an expansion of the FOIA/EIR right of access to information on request. The Government is also keen to see that the economic value of public sector information is fully exploited.
74. As far as privacy is concerned, the aim is to reduce the extent to which central and local Government keep individuals under observation and collect information about them. There is however little sign so far of any intention to address the collection and use of personal information by commercial organisations, or by the media.
75. The Programme makes clear that the Government's first priority is to reduce the budget deficit, and that everything else takes second place. We can expect that the various proposals discussed above will be rapidly implemented where they involve immediate savings, but not where they would require further expenditure. It is likely that the public authorities will be expected to do more in terms of giving access to information that they hold, but without being given additional money to do so, and without there being any additional resources for regulators (e.g. the Information Commissioner) to enforce these new obligations.

⁴¹ See http://www.ipt-uk.com/docs/IPT_03_32_H.pdf

76. 11KBW's Panopticon blog (<http://www.panopticonblog.com/>) will be following the progress of the new Government's agenda: please visit the blog for news about the latest developments.

May 2010